OCPP Certification Program

Document 2

Test Procedure & Test Plans

2020-03-31

V1.0.2

Open Charge Alliance | Utrechtseweg 310 - Building B42 | 6812 AR Arnhem, The Netherlands

Contents

1. Introduction

This document describes the test procedure and the test plans of the OCPP Certification Program.

The test procedure covers testing of:

- a Charging Station
- a Charging Station Management System (CSMS)

Currently the OCPP version eligible for certification is:

- OCPP 1.6 edition 2
- (Certification for OCPP 2.0 will follow later)

2. Terms and definitions

Term / abbreviation	Definition / description
Certification Profile	A set of OCPP functionalities developed by the OCA to target the needs of a specific business driver accredited by the Alliance.
Charging Station	Refers to a Charge Point (OCPP 1.6 terminology) or Charging Station (OCPP 2.0 terminology)
CSMS	Central System (OCPP1.6 terminology) or Charging Station Management System (OCPP2.0 terminology)
Device	An OCPP based device eligible for OCPP certification. In this document, this refers to a Central System or a Charge Point.
DUT	Device Under Test: The device submitted by the vendor for OCPP certification.
OCA	Open Charge Alliance
Participants	Any company involved in the OCPP certification program.
PICS	Protocol Implementation Conformance Statement. The completed PICS document is provided by the vendor to the Test Laboratory, asserting which OCPP specific requirements are met by its device.
Test Laboratory	An independent test laboratory authorized by the Open Charge Alliance to administer the approved OCPP tests and to assess eligibility of devices for OCPP certification.
Vendor	A manufacturer / developer submitting devices for certification.

3. References

No	Title
1	OCPP Certification Procedure

4. Test overview

4.1 Test coverage

To become OCPP certified, the tested Device Under Test (DUT), has to successfully pass the following parts:

- **Conformance tests:** the tested DUT is tested against the OCPP Compliance Testing Tool. The tool has built in validations that should not fail during certification tests. With these validations the Tool verifies whether the DUT has implemented the OCPP specification correctly. The optional features of the OCPP protocol are also covered by the certification, if supported by the DUT. The set of optional features is listed in appendix C.
- **Performance measurements:** a number of performance values of the tested DUT are measured and give an idea how the device behaves in a lab environment. The performance parameters are stated by the vendor in the Protocol Implementation Conformance Statement (PICS).

4.2 Test prerequisites

The following prerequisites are applicable for certification testing:

- A Protocol Implementation Conformance Statement (PICS) has to be completed by the vendor of a DUT when submitting a solution for OCPP certification (See Appendix A: Protocol Implementation Conformance Statement). This should include all relevant limits and non-OCPP settings that are relevant for the test laboratory and for the correct functioning of the Charging Station / CSMS.
- As a part of the certification process, the test lab will verify the PICS and in case of a Charging Station, all configuration keys will be read, validated where applicable and added to the test report.
- For CSMS:
    - The vendor shall supply either a running copy of a CSMS on a server / laptop to the test laboratory or give the test laboratory access to a running copy of the CSMS on a separate environment that is accessible via the Internet (e.g. a cloud environment). In the latter case, an Internet connection from the test laboratory to the CSMS shall be made available. This environment shall be “handed over” to the test laboratory and not updated by the vendor without knowledge of the test laboratory.
- For Charging Station:
    - A network connection to the Charging Station should be available via a telecom connection or wired ethernet connection.
    - To be able to test actual transactions, an EV is needed or has to be simulated. In the current EV market multiple types of sockets exist and no affordable EV simulators for all types of sockets are available at the time of writing. If an EVSE tester is available, this can be used (e.g. a type 2 socket to regular household socket with a dummy device (e.g. heater)). If no EV test socket or other test device is available at the testlab for a socket type, an EV is used. Please refer to Appendix E for examples of EVs that could be used per socket type.
- A technical representative of the Vendor is allowed to participate to the tests. If not physically present, a remote support from the technical team of the vendor

must be arranged between the vendor and the test laboratory to help solving any issue raised during the certification tests.
- A Charging Station that supports more than 1 security profile, has to be delivered with the lowest supported security level. During certification it will be upgraded.
- To successfully execute the mandatory conformance test cases, the prerequisites for these tests have to be met.

5. Test procedure and Responsibilities

5.1 Certification Documents & Support

Test plans, configuration guides and engineering support are made available by the Test Laboratory to vendors in all stages of a vendor's preparation for certification. The responsibility for the test plans lies with the Open Charge Alliance.

5.2 Test Instrumentation & Test Plan

The Test Laboratory will distribute information to vendors regarding the test instruments that will be used during the certification tests if requested.

5.3 Test Procedures

Testers of the test laboratory will execute all tests and test procedures adhering strictly to the OCPP tests plans. Engineering staff from vendor companies may be present. Their presence may be required to resolve issues that may arise in the course of testing.

5.4 Pass Criteria

To be certified a vendor must successfully pass all tests described in chapter 4 and as defined in the OCPP test plans for the CSMS or Charging Station submitted for certification.

In exceptional cases (e.g. in case of bugs in OCPP Compliance Testing Tool) the OCA Compliance Working group can decide that a vendor is certified despite not passing all tests according to the test plans.

5.5 Retesting

Testers of the test laboratory will execute all tests and test procedures that are applicable for the Protocol Implementation Conformance Statement (PICS) that is reported by the vendor prior to the certification. If one or more tests fail, this will be reported back to the vendor and no certificate will be awarded (yet).

The policy for re-testing for the certification testing by the test laboratories is described below.

- Certificates are only valid for the device tested by the test laboratories and apply for a specific hardware feature set and a specific OCPP software version;
- It is not allowed during the test to manually change the configuration. In that case all certification tests should be started over again;
- Any change on the device (hardware feature set or OCPP software version) during the course of testing is not allowed and will require a full re-test of the DUT by the test laboratory;
- If a device “crashes” and requires a reset during conformance testing, this is considered as failing the conformance tests (and thus certification) and will thus require a re-test of the certification laboratory. This excludes crashes or problems caused by improper handling of the device by the test laboratory.

In case of un-clarity regarding the re-testing procedure, only the CWG of the Open Charge Alliance is authorized to decide on the procedure to be followed and this is not to be discussed between the Test Laboratory and the vendor.

5.6 Issue handling

Handling issues during tests can be separated in the following types:

- Configuration / setup issues. These are solved during testing, if necessary with the help of the technical representative of the vendor. When during the testing of a device a non-OCPP configuration is changed, all certification tests should be started over again;
- Bugs in software / hardware. This is considered as failing the certifications tests. See also 5.5 for handling of this situation.

6. Test Setup

6.1 General setup

The test setup used for Conformance testing is similar to the setup for the performance measurements. In order to have a fair comparison the connection properties are measured as part of the test. The test setups for testing are displayed in Figure 1 to Figure 3.

In Figure 1 the setup for a CSMS with a fixed ethernet connection is displayed. The CSMS is connected to the internet as well as the machine running the OCPP Compliance Testing Tool. Before starting the actual tests, the bandwidth as well as the latency for the network connection are measured. Please refer to the next paragraph for more information on the Test laboratory connection tester.

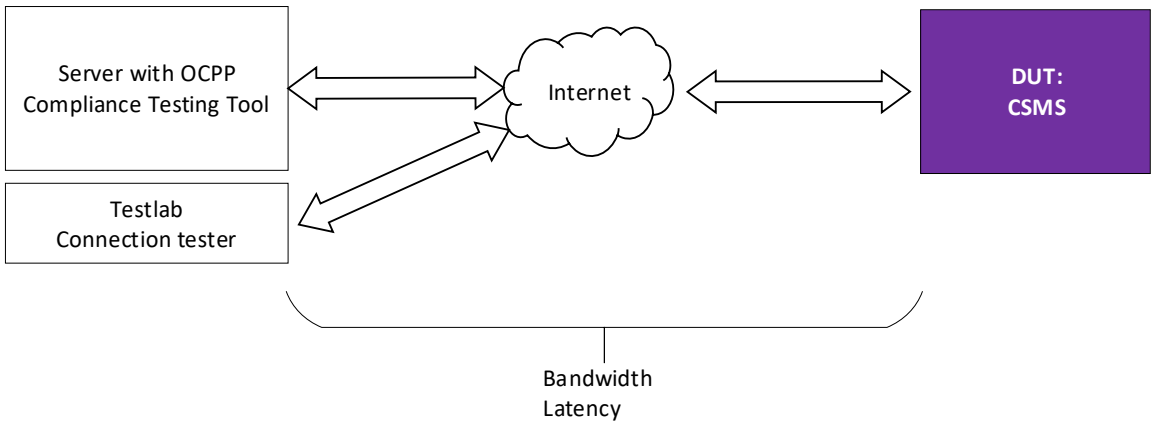

Figure 1: CSMS with fixed ethernet connection

In Figure 2 the setup for a Charging Station with a fixed ethernet connection is displayed. The Charging Station is connected via a UTP cable to the Charging Station. To be able to test actual transactions, actual EVs, EV test sockets or other test devices are used. In the current EV market multiple types of sockets exist and no affordable EV simulators for all types of sockets are available at the time of writing. For this reason, if no EV test socket or other test device is available at the testlab, an EV is to be used (e.g. rented). Please refer to Appendix E for examples of EVs to use per socket type.

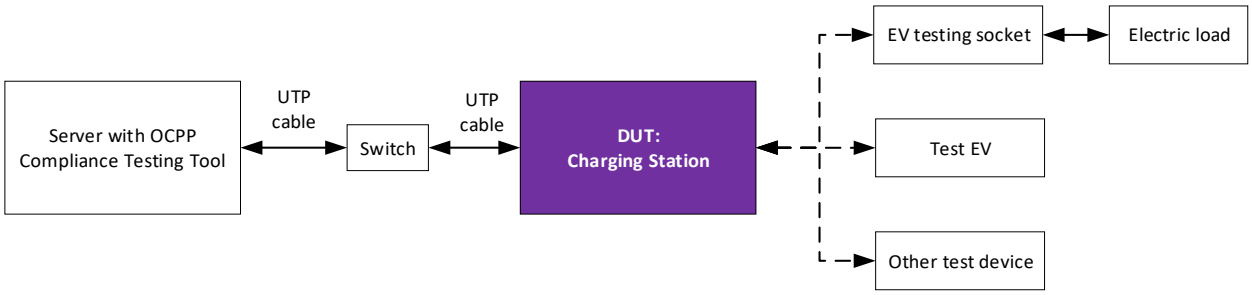

Figure 2: Charging Station with fixed ethernet connection

In Figure 3 the setup for a Charging Station with a telecom-only connection is displayed. The Charging Station is connected via mobile network to the OCPP Compliance Testing Tool. To be able to test bandwidth, 2 SIM cards (same network operator) are used: 1 for the Charging Station under test and 1 for testing the mobile internet connection at that location, with a Testlab Connection tester. A prerequisite for SOAP connections is to use SIM cards that use a fixed public IP address. Since this is easier for whitelisting purposes for JSON connections at the testlabs, this is also used for JSON Charging Stations. The SIM cards will be provided by the test labs.

To be able to test actual transaction, test sockets / test devices are used (see explanation above).

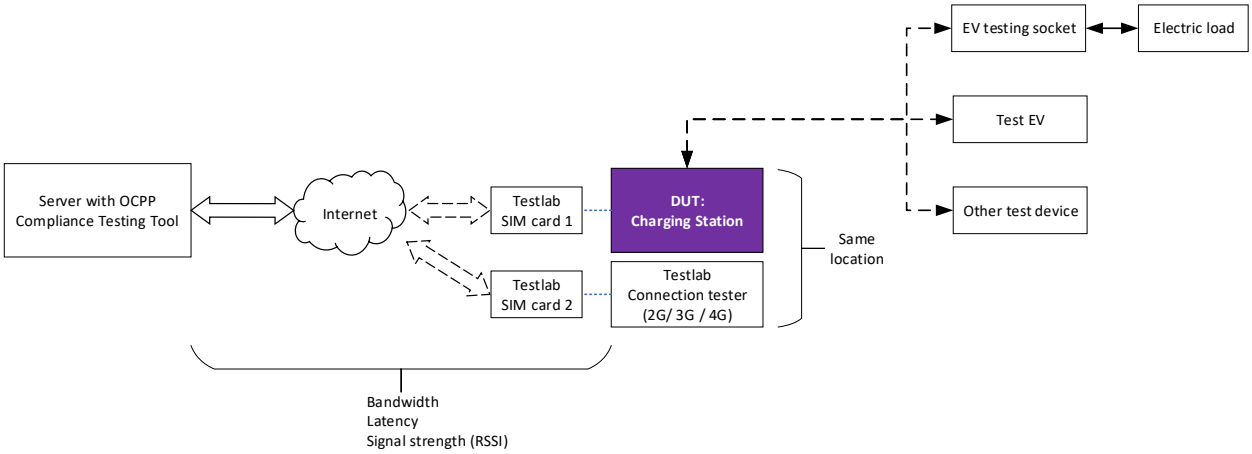

Figure 3:Charging Station with (only) telecom connection

For the tests where the DUT is a Charging Station, the OCA will provide test RFID cards that can be used in combination with the OCPP Compliance Testing Tool.

6.2 Test laboratory tools

The Test laboratory will use the following test tools:

- EVSE tester plug for AC type 1
- EVSE tester plug for AC type 2
- EV simulator / test socket for DC charging (tbd)
- Mobile communication dongle that supports enabling and disabling 2G, 3G and 4G
- OCPP Compliance Testing Tool (OCTT)
- Test laboratory connection tester

Test laboratory connection tester

The test laboratory shall use a "connection tester", which refers to hardware / software that can measure:

- the internet connection from the server with OCPP Compliance Testing Tool to the CSMS under test. This will be done by executing an online internet speed test on both the CSMS as well as the machine running the OCPP Compliance Testing Tool.
- the properties of the internet connection (2G and / or 3G and / or 4G) from the server with OCPP Compliance Testing Tool to the location of the Charging Station under test.
  This can for example be done by using a mobile communication dongle and a laptop. This dongle must support enabling and disabling 2G, 3G and 4G. For each type, an online internet speed test will be executed, to determine the bandwidth / latency. For determining the signal strength, separate software could in this setup be used to determine the signal strength (actual results depends on the dongle used, but it is merely to get an indication of the signal strength).
  For uniformity, the same device is to be used for this by all labs. Please refer to Appendix B for the exact device that will be used.

7. Conformance test plan

7.1 Introduction

This chapter describes the conformance test plan for vendors to successfully complete as part of the OCPP certification program.

7.1.1 Objective

The objective of the conformance tests is to verify and validate the correct implementation of the OCPP protocol of a Charging Station or CSMS.

7.1.2 Scope of tests

The scope of the conformance tests is to verify and validate the correct implementation of the OCPP protocol of a Charging Station or CSMS by testing the DUT against the OCPP Compliance Testing Tool (OCTT) which automatically validates the responses by the DUT. Furthermore, the basic functionalities that are a consequence of messages in the OCPP protocol of a Charging Station or CSMS are verified and validated during these OCTT tests.

These tests are done by doing manual checks while running scenarios from the OCPP Compliance Testing Tool.

7.1.3 Acceptant and acceptance criteria

The Test Laboratory that executes the conformance test is not responsible for accepting or rejecting an OCPP implementation, but only responsible for executing the conformance test and reporting the results to the vendor and OCA.

The acceptance criteria for the conformance test is that all mandatory and applicable conditional tests for certification are executed successfully.

7.1.4 Optional functionalities within feature profiles

OCPP holds some optional Charging Station functionalities within the enclosed environment of a feature profile. These functionalities are managed by Read-only / Optional Configuration Keys. A issued certificate contains the following information:

- Whether the optional configuration keys are implemented or not.
- What value the implemented “Read-only” configuration keys contain.
- Description of the functionalities belonging to the configuration keys.

7.2 Conformance tests

7.2.1 Test basis

OCPP 1.6

The basis for testing conformance is the OCPP 1.6 edition 2 specification (date: 2017-09-28), OCPP 1.6 Errata sheet v4.0 Release (date: 2019-10-23) and OCPP 1.6 security whitepaper ed2 (date: 2020-03-31)

Additionally, the following documentation is used:

- the scenarios for conformance testing are documented in Appendix C: List of conformance tests. This list contains the list of mandatory and conditional scenarios from the OCPP Compliance Testing Tool.

OCPP 2.0

- *To be determined.*

7.2.2 Test approach

The approach of testing is to test the DUT using the OCPP Compliance Testing Tool, manual functional verifications are executed during these conformance tests. Between tests, a utility test case (000_RESET) from the OCPP Compliance Testing Tool is used (and must pass) to set the Charging Station to a basic idle state to prevent test cases influencing each other.

The overall test process consists of the following steps:

- The Internet connection properties are measured.
- Test scenarios are started automatically using the OCPP Compliance Testing Tool.

- Most messages are automatically exchanged.
- Manual actions are executed by a test laboratory tester.
- Manual / on screen validations are executed by a test laboratory tester.

Intake DUT

As part of the conformance test, the following intake is done:

- A short pre-test is done to show that the DUT is functioning and is not, for example, damaged during transport.
- As an input the vendor should indicate whether or not the DUT supports sending milliseconds in OCPP messages.

Entry and exit criteria

Entry criteria for executing conformance test:

- All prerequisites that are documented in the OCPP Certification Procedure shall be met.
- All prerequisites that are documented in the OCPP Certification Test Procedure shall be met.
- Sufficient documentation about the DUT is available to the test laboratory in order to execute the manual actions for the test scenarios.

Exit criteria for executing conformance test:

- All mandatory test scenarios from Appendix C shall be executed successfully.

7.3 Test script

The actions that are executed for the conformance tests are the following:

Preparation:

1. The OCPP Compliancy Testing Tool is installed (once)
2. The OCPP Compliancy Testing Tool is started and the UI opened in a browser[1]
3. Fill in the test configuration in the "OCPP Certification Report".
    a. It is recommended that testcase 019 is used for this. It will retrieve all implemented configuration keys.
    b. The value of the "Read-only" Configuration keys can be immediately taken over in the test configuration table.
    c. The "Read-write" configuration keys should be written down while testing. Different values may be used for each test. So they are able to contain multiple values, depending on the executed tests and the used tool configurations.

Execution will be done for each test from Appendix C:

1. If testing a Charging Station:
    a. The charging station is returned to basic state of operations using the OCTT test case id 000_RESET (must be executed *successfully* before continuing)
2. If a transaction is running, the transaction is manually stopped or stopped using OCTT test case id 000_STOPTX
3. The test case no (column "No. from appendix A) is started in the OCTT. The Id used in the test tool user interface is indicated in the column OCTT Id in Appendix C.
4. The steps in the scenario details in the Test case document of the OCPP Compliance Testing Tool and the instructions given by the tool user interface are followed. If the DUT is a Charging Station, the OCTT will execute the steps in the column "Central System (Tool)", if the DUT is a CSMS, the OCTT will execute the steps in the column "Charge Point (Tool)". Tool validations are done automatically.
5. If applicable for the test case when testing a Charging Station):
    a. The StatusNotifications that are received by the OCTT are manually validated (see Appendix D for the OCTT Test Rules).
6. After finishing the test case in the OCTT: based on the outcome of the test (PASS / FAIL) and the OCTT test rules (see Appendix D), the result of the scenario is determined.
7. The Test Report is updated accordingly.

[1] For the firmware update test, the timeout should be adjusted.

8. Performance measurements

8.1 Introduction

This chapter describes the performance measurements that are performed by the test laboratory as part of the OCPP certification program.

8.1.1 Objective

The objectives of the Performance measurements are to measure the performance of a DUT within a lab context and to provide these as additional information to the certificate. The purpose of the Performance measurement is to measure the performance parameters that are stated by a vendor in the Protocol Implementation Conformance Statement (PICS).

8.1.2 Scope of tests

The scope of the performance measurement is to measure a number of performance parameters that are stated by a vendor in the Protocol Implementation Conformance Statement (PICS). For the example template for a PICS related to performance, please refer to Appendix A.4. The values that are stated by the vendor in the PICS do not have to fall within a set of upper / lower boundaries for certification, but will only be included in the test report to provide information to buyers of a device. These performance parameters are listed in paragraph 8.2.1.

8.1.3 Acceptant and acceptance criteria

The Test Laboratory that executes the performance measurement is not responsible for accepting or rejecting an OCPP implementation, but only responsible for executing the performance measurement and reporting the results to the vendor and OCA.

The only acceptance criterium for the performance measurement is that all parameters from the PICS are measured.

8.2 Performance measurements

8.2.1 Test basis

OCPP 1.6

The basis for the measurements is the OCPP 1.6 edition 2 specification (date: 2017-09-28), OCPP 1.6 Errata sheet v4.0 Release (date: 2019-10-23) and OCPP 1.6 security whitepaper ed2 (date: 2020-03-31).

The following list of performance parameters is used:

Name	Description
OCPP triggered function timeout	The timeout used for when waiting for an OCPP function with its corresponding request message (e.g. time between receiving RemoteStartTransaction.conf and StartTransaction.req). Messages to the DUT can be handled within this timeout. This value excludes firmware, diagnostics and rebooting (e.g. based on a reset)
OCPP response timeout	The timeout used for when waiting for an OCPP response message. Messages to the DUT can be handled within this timeout.
Response time Authorize	The response time for the Authorize message.
Response time RemoteStartTransaction	The response time for the RemoteStartTransaction message.

OCPP 2.0

To be determined.

8.2.2 Test approach

Performance measurements will be done in the following way: for measuring message timeouts the OCPP Compliance Testing Tool for OCPP is used. This tool logs all messaging. Based on this logging, the response times are determined.

As introduced in chapter 6, the tests are executed in a predefined test setup. Especially for performance measurements, this setup is important to get accurate measurements. Furthermore; it is important to measure performance in detail, without including effects that are out of control of a DUT.

In case of the OCPP protocol the main bottleneck is the network connection between the Charging Station and the CSMS. For this reason a number of parameters related to bandwidth is measured in (and by) the test laboratory before and during the measurement when a mobile connection is used. This is done using a mobile communication dongle connected to a laptop at the same location. This is (of course) only an indication to make sure that the mobile communication network is available at that location.

The following table lists the parameters that are measured concerning the network connection:

Parameter	Unit	Minimum / maximum for test setup*
Bandwidth	kB per second	Minimum: 5 kB per second
Latency	ms	Maximum: 1000 ms
Signal strength (RSSI) if applicable	dBm	Minimum: -81 dBm (CSQ 16)

* If these values are not met, the test lab should change the setup to improve the connection, before executing the measurement.

Please note: only 1 communication technology is measured for performance, so if multiple technologies available in a Charging Station, the technology that has to be used for the measurements must be stated in the PICS for performance.

8.2.3 Intake DUT

As part of the performance measurement, the following intake is done:

- Connectivity between the OCPP Compliance Testing Tool to the DUT is setup and measured (bandwidth, latency, RSSI).
- If not done during previous tests, a short pre-test is done to show that the DUT is functioning and is not, for example, damaged during transport.

8.2.4 Entry and exit criteria

Entry criteria for executing performance measurements:

- All prerequisites that are documented in the OCPP Certification Procedure shall be met.
- All prerequisites that are documented in the OCPP Certification Test Procedure shall be met.
- Sufficient documentation about the DUT is available to the test laboratory in order to execute the manual actions for the test scenarios.

Exit criteria for executing performance measurements:

- All performance criteria that are listed in 8.2.1 shall be measured.

8.3 Test script

The actions that are executed for the performance measurements are the following:

Preparation for a Charging Station:

1. The Charging Station that is tested, must be configured in the OCPP Compliance Testing Tool.
2. The network parameters as described in paragraph 8.2.2 are measured. In case of a poor network connection, it is attempted to optimize the connection so that it does not influence the performance measurements results.

Preparation for a CSMS:

1. The CSMS must be configured in the OCPP Compliance Testing Tool.
2. The network parameters as described in paragraph 8.2.2 are measured. In case of a poor network connection, it is attempted to optimize the connection so that it does not influence the performance measurements results.

For the timeout values, the OCPP Compliance Testing Tool logs are used to determine the measured values. The Test Report is updated accordingly.

Appendix A: Protocol Implementation Conformance Statement

There are three PICS:

1. PICS for OCPP1.6
2. PICS for OCPP1.6 Security
3. PICS for OCPP1.6 Performance Measurement

The PICS for OCPP2.0 will be determined at a later date.

General information about DUT

The following table should list the general information about the DUT:

Vendor name	<>
DUT	CSMS / Charging Station
Communication	SOAP / JSON
Type / model (for CS only)	<type name and / or model number>
Socket(s) / connector(s) (for CS only)	Singe / multiple
Fixed cable (for CS only)	<Yes / No>
OCPP Software version	<version>
Support for milliseconds in OCPP messages	Yes / No
Communication technology	WiFi / ethernet / mobile network
RFID readers	none / single /one per EVSE

Optional features

The following table should list the presence / absence of some optional features:

Feature	Supported / present
Authorization Cache	Yes / No
Unknown Offline Authorization ***MaxEnergyOnInvalidId***	Yes / No *Yes / No*
MinimumStatusDuration	Yes / No If supported by a Charging Station, the station is to be delivered to the test lab with the value set to 0.
WebSocketPingInterval (only for websocket implementations)	Yes / No
Support reservations of entire Charging Station	Yes / No
Choice transaction stopped when cable disconnected on EV side	Yes / No

Other relevant settings and limits

The table below should contain all relevant limits and non-OCPP settings that are relevant for the test laboratory and for the correct functioning of the Charging Station / CSMS:

Limit / setting	Value
GetConfigurationMaxKeys	…
MeterValuesAlignedDataMaxLength	…
MeterValuesSampledDataMaxLength	…
Minimum MeterValueSampleInterval supported	…
Maximum MeterValueSampleInterval supported	…
Minimum HeartbeatInterval supported	…
Maximum HeartbeatInterval supported	…
StopTransactionMaxMeterValues	…
StopTxnAlignedDataMaxLength	…
StopTxnSampledDataMaxLength	…
WebSocketPingInterval	…
Local Authorization List	
LocalAuthListMaxLength	…
SendLocalListMaxLength	…
Smart charging	
ChargeProfileMaxStackLevel	…
ChargingScheduleAllowedChargingRateUnit	<list>
ChargingScheduleMaxPeriods	…
Firmware Management	
Supported file transfer protocols	{http, https, ftp, ftps}
Other relevant values	
<other minimum value>	…
<other maximum value>	…

IP configuration

The test laboratory will provide information on the network configuration that has to be configured on the Charging Station beforehand.

A.1 PICS OCPP 1.6 certificate

The Table below states the mandatory and optional functionalities for certification. When a functionality is supported by the DUT, all applicable use cases must be supported, unless stated otherwise.

Name	OCPP 1.6 Fully supported	OCPP 1.6 Subset supported	Description
Core	Yes	Yes	Basic Charging Station functionality for booting,

			authorization (incl. cache if available), configuration, transactions, remote control.
Included functionalities			
	Cold Boot Charge Point		
	Cold Boot Charge Point		
	Cold Boot Charge Point - Pending		
	Start Charging Session		
	Regular Charging Session - Plugin First		
	Regular Charging Session – Identification First		
	Regular Charging Session – Identification First - ConnectionTimeOut		
	Stop Charging Session		
	Stop transaction - IdTag in StopTransaction matches IdTag in StartTransaction		
	Stop transaction - ParentIdTag in StopTransaction matches ParentIdTag in StartTransaction		
	EV Side Disconnected		
	One Reader for Multiple Connectors		
	One Reader for Multiple Connectors (optional)		
	Cache (if available)		
	Regular Start Charging Session – Cached Id		
	Clear Authorization Data in Authorization Cache		
	Transaction Related Message not Accepted by Central System		
	Core Profile - Remote actions Happy Flow		
	Remote Start Charging Session – Cable Plugged in First		
	Remote Start Charging Session – Remote Start First		
	Remote Start Charging Session – connection timeout		
	Remote Stop Charging Session		
	Core Profile - Resetting Happy Flow		
	Hard Reset Without transaction		
	Soft Reset Without Transaction		
	Hard Reset With Transaction		
	Soft Reset With Transaction		
	Core Profile - Unlocking Happy Flow		
	Unlock connector - no charging session running(Not fixed cable)		
	Unlock connector - no charging session running(Fixed cable)		
	Unlock Connector - With Charging Session		
	Core Profile - Configuration Happy Flow		
	Retrieve configuration (Charging Station only)		
	Retrieve all configuration keys (CSMS only)		
	Retrieve specific configuration key (CSMS only)		
	Change/set Configuration		
	Meter values		
	Sampled Meter Values		

	Clock-aligned Meter values		
	Core Profile - Basic Actions Non-happy Flow		
	Start Charging Session – Authorize invalid / blocked / expired		
	Start Charging Session Lock Failure		
	Send Local Authorization List - NotSupported		
	Get Local List Version - NotSupported		
	Core Profile - Remote Actions Non-Happy Flow		
	Remote Start Charging Session – Rejected		
	Remote Stop Transaction – Rejected		
	Core Profile - Unlocking Non-happy Flow		
	Unlock Connector – Unlock Failure		
	Unlock Connector – Unknown Connector		
	Core Profile - Power Failure Non-Happy Flow		
	Power failure boot charging point-configured to stop transaction(s)		
	Power Failure with Unavailable Status		
	Core Profile - Offline behavior Non-Happy Flow		
	Connection Loss During Transaction		
	Offline Start Transaction		
	Offline Stop Transaction		
	Offline Transaction		
	Core Profile - Configuration Keys Non-Happy Flow		
	Configuration keys		
	DataTransfer		
	Data Transfer to a Charge Point		
	Data Transfer to a Central System		
Firmware Management	**Yes**	**Yes / No**	**Support for (remote) firmware update management and diagnostic log file download.**
Included functionalities			
	Firmware Management		
	Firmware Update - Download and Install		
	Firmware Update - Download Failed		
	Firmware Update - Installation Failed		
	Diagnostics		
	Get Diagnostics		
	Get Diagnostics - Upload Failed		
Smart Charging	**Yes**	**Yes / No**	**Support for Smart Charging (all profile types, including stacking), to control charging.**
Included functionalities			

	Central Smart Charging		
	Central Smart Charging - TxDefaultProfile		
	Central Smart Charging - TxProfile		
	Central Smart Charging - No ongoing transaction		
	Central Smart Charging - Wrong transactionId		
	Central Smart Charging - TxDefaultProfile - with ongoing transaction		
	Get Composite Schedule		
	Clear Charging Profile		
	Stacking Charging Profiles		
	Remote Start Transaction with Charging Profile		
	Remote Start Transaction with Charging Profile		
	Remote Start Transaction with Charging Profile - Rejected		
Reservation	**Yes**	**Yes / No**	**Support for reservation of a connector of a Charging Station.**
Included functionalities			
	Reservation of a Connector		
	Reservation of a Connector – Local start transaction		
	Reservation of a Connector – Remote start transaction		
	Reservation of a Connector - Expire		
	Reservation of a Connector - Occupied		
	Reservation of a Connector - Unavailable		
	Reservation of a Connector - Rejected		
	Reservation of a Charge Point		
	Reservation of a Charge Point - Transaction		
	Reservation of a Charge Point - Occupied		
	Reservation of a Charge Point - Unavailable		
	Cancel Reservation		
	Cancel Reservation		
	Cancel Reservation - Rejected		
	Use a reserved Connector with parentIdTag		
Local Authorization List Management	**Yes**	**Yes / No**	**Features to manage a local list in the charging station containing authorization data for whitelisting users.**
Included functionalities			
	Get Local List Version		
	Get Local List Version (empty)		
	Send Local Authorization List		
	Send Local Authorization List		
	Send Local Authorization List - VersionMismatch		
	Send Local Authorization List - Failed		

	Send Local Authorization List - Full		
	Send Local Authorization List - Differential		
	Regular Start Charging Session – Id in Local Authorization List		
Remote Trigger	**Yes**	**Yes / No**	**Support for remotely triggering messages that originate from a Charging Station. This can be used for resending messages or for getting the latest information from the Charging Station.**
Included functionalities			
	Trigger Message		
	Trigger Message - Rejected		

A.2 PICS OCPP 1.6 security certificate

Security extension (based on whitepaper, JSON only).

Supported cipher suites (Charging Station only)[2]

Cipher suite	Supported
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 AND TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	Yes / No
TLS_RSA_WITH_AES_128_GCM_SHA256 AND TLS_RSA_WITH_AES_256_GCM_SHA384	Yes / No

Certificate Profiles

Name	Implemented	Description
Security Profile 1	Yes / No	**Unsecured Transport with Basic Authentication** Profile 1 is optional
	Secure connection setup	
	Update Charge Point Password for HTTP Basic Authentication	
	Security event/logging	
	Get Security Log	
	Secure firmware update	
	Secure Firmware Update	
	Secure Firmware Update - Invalid Signature	
Security Profile 2	Yes / No	**TLS (1.2 or higher) with Basic Authentication** Security profile 2 or security profile 3 or both must be implemented
	Secure connection setup	
	Update Charge Point Password for HTTP Basic Authentication	
	Install a certificate on the Charge Point	
	Delete a specific certificate from the Charge Point	
	Security event/logging	
	Invalid CentralSystemCertificate Security Event	
	Get Security Log	
	Secure firmware update	
	Secure Firmware Update	
	Secure Firmware Update - Invalid Signature	
Security Profile 3	Yes / No	**TLS (1.2 or higher) with Client Side Certificates** Security profile 2 or security profile 3 or both must be implemented

[2] Please note that the CSMS SHALL support at least the following four cipher suites: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_256_GCM_SHA384

	Secure connection setup
	Update Charge Point Certificate by request of Central System
	Install a certificate on the Charge Point
	Delete a specific certificate from the Charge Point
	Security event/logging
	Invalid ChargePointCertificate Security Event
	Invalid CentralSystemCertificate Security Event
	Get Security Log
	Secure firmware update
	Secure Firmware Update
	Secure Firmware Update - Invalid Signature

Besides filling the above table, the vendor must also supply (examples of) the public certificates that will be used during the tests, in order to prepare the tests at the test lab.

A.3 PICS OCPP 2.0 certificate

To be determined.

A.4 PICS for OCPP 1.6 performance measurement (OCPP2.0 t.b.d.)

Name	Value	Unit	Description
OCPP triggered function timeout (Charging Station only)	XX	seconds	The response time for when waiting for an OCPP function with its corresponding request message. (Firmware update, Diagnostics and Reboot are excluded from this measurement.) ***Message combinations checked:*** *CancelReservation / StatusNotification(status=Available)* *ReserveNow / StatusNotification(status=Reserved)* *ChangeAvailability / StatusNotification* *RemoteStartTransaction / StatusNotification(status=Preparing) OR Authorize OR StartTransaction* *RemoteStopTransaction / StopTransaction* *TriggerMessage / <Triggered Message>*
OCPP response timeout	XX	seconds	The response time for when waiting for an OCPP response message.
Response time Authorize (CSMS only)	XX	seconds	The response time for the Authorize message.
Response time RemoteStartTransaction (Charging Station only)	XX	seconds	The response time for the RemoteStartTransaction message.

The communication technology for which the measurements are done:

Communication technology	<WiFi / ethernet / mobile>

Please note: only 1 communication technology is measured for performance, so if multiple technologies availavle in a Charging Station, please select for which the measurements should be executed by the lab.

Appendix B: Test tools

The following tools are used during the certification tests:

- OCPP Compliance Testing Tool. This test tool is supplied to the Testing Laboratory and maintained by the Open Charge Alliance.
- Mobile communication dongle for performance measurements
    - Brand: Huawei
    - Type: E3372h LTE dongle
- EV emulator, the following types will be used
    - EV emulator for AC / DC Type 1
        - Brand: T.b.d.
        - Type: T.b.d.
    - EV emulator for AC / DC Type 2
        - Brand: T.b.d.
        - Type: T.b.d.

Appendix C: List of conformance tests

OCPP 1.6 (Full & Subset)

M = Mandatory

O = Optional

C = Conditional (condition in the “Remark” column)

No	OCTT Id	OCPP Compliance Testing Tool scenario	Conf. Test for Charging Station	Conf. test for Central System	Remark
		CORE			
		Cold Boot Charge Point			
1	_001	Cold Boot Charge Point	M		
2	_002	Cold Boot Charge Point - Pending	M	O	
3	_000_BOOT	Send Boot Notification to Central System		M	
		Start Charging Session			
4	_003	Regular Charging Session - Plugin First	C	M	Only applicable for a Charge Point which supports local start/stop transaction.
5	_004_1	Regular Charging Session – Identification First	C	M	Only applicable for a Charge Point which supports local start/stop transaction.

6	_004_2	Regular Charging Session – Identification First - ConnectionTimeOut	C	M	Only applicable for a Charge Point which supports local start transaction.
		Stop Charging Session			
7	_068	Stop transaction - IdTag in StopTransaction matches IdTag in StartTransaction	C		Only applicable for a Charge Point which supports local start/stop transaction.
8	_069	Stop transaction - ParentIdTag in StopTransaction matches ParentIdTag in StartTransaction	C		Only applicable for a Charge Point which supports local start/stop transaction.
9	_005_1	EV Side Disconnected	C	M	StopTransactionOnEVSideDisconnect = true, UnlockConnectorOnEVSideDisconnect = true Condition: The Charge Point does not have a fixed cable on Charge Point side AND The configuration key StopTransactionOnEVSideDisconnect does NOT have the accessibility ReadOnly in combination with value false.
10	_005_2	EV Side Disconnected	C		StopTransactionOnEVSideDisconnect = true, UnlockConnectorOnEVSideDisconnect = false Condition: The configuration key StopTransactionOnEVSideDisconnect does NOT have the accessibility ReadOnly in combination with value false.
11	_005_3	EV Side Disconnected	C		StopTransactionOnEVSideDisconnect = false, UnlockConnectorOnEVSideDisconnect = false Condition:

					The configuration key StopTransactionOnEVSideDisconnect is implemented AND has the accessibility ReadWrite
		One Reader for Multiple Connectors			
12	_006	One Reader for Multiple Connectors	O		Only applicable for a Charge Point with one reader for multiple Connectors and optional / not blocking for certification, since it is not explicitly in the specification.
		Cache			
13	_007	Regular Start Charging Session - Cached Id	C	M	Only applicable if a cache is available.
14	_061	Clear Authorization Data in Authorization Cache	C	M	Only applicable for a Charge Point which supports local start/stop transaction AND if a cache is available.
		Core Profile - Remote actions Happy flow			
16	_010	Remote Start Charging Session - Cable Plugged in First	M	M	
17	_011_1	Remote Start Charging Session - Remote Start First	M	M	
18	_011_2	Remote Start Charging Session - connection timeout	M	M	
19	_012	Remote Stop Charging Session	M	M	
		Core Profile - Resetting Happy Flow			
20	_013	Hard Reset Without transaction	M	M	
21	_014	Soft Reset Without Transaction	M	M	
22	_015	Hard Reset With Transaction	M		
23	_016	Soft Reset With Transaction	M		

		Core Profile - Unlocking Happy flow			
24	_017_1	Unlock connector - no charging session running (Not fixed cable)	C	M	Only applicable for a Charge Point with a detachable cable.
25	_017_2	Unlock connector - no charging session running (Fixed cable)	C	M	Only applicable for a Charge Point with a fixed cable.
26	_018_1	Unlock Connector - With Charging Session (Not fixed cable)	C		Only applicable for a Charge Point with a detachable cable.
27	_018_2	Unlock Connector - With Charging Session (Fixed cable)	C		Only applicable for a Charge Point with a fixed cable.
		Core Profile - Configuration Happy flow			
28	_019	Retrieve configuration	M		
29	_019_1	Retrieve all configuration keys		M	
30	_019_2	Retrieve specific configuration key		M	
31	_021	Change/set Configuration	M	M	
		Meter values			
32	_070	Sampled Meter Values	M		
33	_071	Clock-aligned Meter values	M		
		Core Profile - Basic Actions Non-happy flow			
34	_023	Start Charging Session - Authorize invalid / blocked / expired	M		
35	_023_1	Start Charging Session - Authorize invalid		M	
36	_023_2	Start Charging Session - Authorize expired		M	

37	_023_3	Start Charging Session - Authorize blocked		M	
38	_024	Start Charging Session Lock Failure	C	M	Only applicable if the Charge Point does not have a fixed cable on Charge Point side.
62	_043_1	Send Local Authorization List - NotSupported	C	O	If not supported by Charging Station.
59	_042_1	Get Local List Version (not supported)	C	O	If not supported by Charging Station.
		Core Profile - Remote Actions Non-Happy Flow			
39	_026	Remote Start Charging Session - Rejected	M	M	
41	_028	Remote Stop Transaction - Rejected	M	O	
		Core Profile - Unlocking Non-happy flow			
42	_030	Unlock Connector - Unlock Failure	O	M	
43	_031	Unlock Connector - Unknown Connector	M	O	
		Core Profile - Power Failure Non-Happy Flow			
44	_032_1	Power failure boot charging point - configured to stop transaction(s) before going down	C	M	Only applicable for a Charge Point configured to stop transaction(s) before going down.
45	_032_2	Power failure boot charging point-configured to stop transaction(s)	C		Only applicable for a Charge Point configured to stop transaction(s) after going down and being back online again.
46	_034	Power Failure with Unavailable Status	M		
		Core Profile - Offline behavior Non-Happy Flow			

48	_036	Connection Loss During Transaction	M		
49	_037_1	Offline Start Transaction	C	M	Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache. Using valid idTag, AllowOfflineTxForUnknownId = true, LocalAuthorizeOffline = true
50	_037_2	Offline Start Transaction	C		Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache. Using invalid idTag, AllowOfflineTxForUnknownId = true, LocalAuthorizeOffline = true, StopTransactionOnInvalidId = false
51	_037_3	Offline Start Transaction	C	M	Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache. Using invalid idTag, AllowOfflineTxForUnknownId = true, LocalAuthorizeOffline = true, StopTransactionOnInvalidId = true
52	_038	Offline Stop Transaction	C		Only applicable for a Charge Point which supports local stop transaction.
53	_039	Offline Transaction	C	M	Only applicable for a Charge Point which supports local start/stop transaction and at least one of the following 3 functionalities: local authorization list feature profile, Unknown Offline Authorization or Authorization Cache.

		Core Profile - Configuration Keys Non-Happy Flow			
54	_040_1	Configuration keys	M	O	Not supported configuration key.
55	_040_2	Configuration Keys	M	O	Incorrect value.
		DataTransfer			
57	_062	Data Transfer to a Charge Point	M	O	Only verifying that the DUT responds (rejecting is ok).
58	_064	Data Transfer to a Central System	O	M	Only verifying that the DUT responds (rejecting is ok).
Local Authorization List Management					
		Get Local List Version			
60	_042_2	Get Local List Version (empty)	M	M	
		Send Local Authorization List			
61	_043	Send Local Authorization List	M		Prerequisite: support for at least 5 idTokens is required.
63	_043_2	Send Local Authorization List - VersionMismatch	M		
64	_043_3	Send Local Authorization List - Failed	O	M	
65	_043_4	Send Local Authorization List - Full		M	
66	_043_5	Send Local Authorization List - Differential		M	
67	_008	Regular Start Charging Session - Id in Local Authorization List	M		
FirmwareManagement					
		Firmware Management			
68	_044_1	Firmware Update - Download and Install	M	M	For interop: check FTP connection
69	_044_2	Firmware Update - Download Failed	M	O	

70	_044_3	Firmware Update - Installation Failed	M	O	
		Diagnostics			
71	_045_1	Get Diagnostics	M	M	For interop: check FTP connection
72	_045_2	Get Diagnostics - Upload Failed	M	O	
Reservation					
		Reservation of a Connector			
108	_046	Reservation of a Connector – Local start transaction		M	
73	_046_1	Reservation of a Connector – Local start transaction	C		Only applicable for a Charge Point which supports local start transaction.
	_046_2	Reservation of a Connector – Remote start transaction	M		
74	_047	Reservation of a Connector - Expire	M	M	
76	_048_2	Reservation of a Connector - Occupied	M	O	
77	_048_3	Reservation of a Connector - Unavailable	M	O	
78	_048_4	Reservation of a Connector - Rejected	O	M	
		Reservation of a Charge Point			
79	_049	Reservation of a Charge Point - Transaction	M	M	
81	_050_2	Reservation of a Charge Point - Occupied	M		
82	_050_3	Reservation of a Charge Point - Unavailable	M		
		Cancel Reservation			
84	_051	Cancel Reservation	M	M	

85	_052	Cancel Reservation - Rejected	M	O	
86	_053	Use a reserved Connector with parentIdTag	M	O	
		RemoteTrigger			
87	_054	Trigger Message	M	M	
88	_055	Trigger Message - Rejected	M	O	
		SmartCharging			
		Central Smart Charging			
89	_056	Central Smart Charging - TxDefaultProfile	M	M	
90	_057	Central Smart Charging - TxProfile	M	M	
91	_058_1	Central Smart Charging - No ongoing transaction	M	O	
92	_058_2	Central Smart Charging - Wrong transactionId	M	O	
93	_082	Central Smart Charging - TxDefaultProfile - with ongoing transaction	M		
94	_066	Get Composite Schedule	M	M	Prerequisite: support for 3 installed profiles with 5 ChargingSchedule periods is required.
95	_067	Clear Charging Profile	M	M	
96	_072	Stacking Charging Profiles	M		Prerequisite: support for 3 stack levels is required.
		Remote Start Transaction with Charging Profile			
97	_059	Remote Start Transaction with Charging Profile	M	M	
98	_060	Remote Start Transaction with Charging Profile - Rejected	M	O	

OCPP 1.6 Security

No	OCTT Id	OCPP Compliance Testing Tool scenario	Conf. Test for Charge Point	Conf. test for Central System	Remark
		Secure connection setup			
99	_073	Update Charge Point Password for HTTP Basic Authentication	C		Only applicable if the Charge Point supports security profile 1 or 2.
100	_074	Update Charge Point Certificate by request of Central System	C	C	Only applicable if the DUT supports security profile 3.
101	_075	Install a certificate on the Charge Point	C	C	Only applicable if the DUT supports security profile 2 or 3.
102	_076	Delete a specific certificate from the Charge Point	C	C	Only applicable if the DUT supports security profile 2 or 3.
		Security event/logging			
103	_077	Invalid ChargePointCertificate Security Event	C	C	Only applicable if the DUT supports security profile 3.
104	_078	Invalid CentralSystemCertificate Security Event	C	C	Only applicable if the DUT supports security profile 2 or 3.
105	_079	Get Security Log	M	M	
		Secure firmware update			
106	_080	Secure Firmware Update	M	M	
107	_081	Secure Firmware Update - Invalid Signature	M	O	

Appendix D: Conformance tests - OCTT Test Rules

The following rules apply:

- If an expected StatusNotification is not received by the OCPP Compliance Testing Tool, the result should not be approved (click No in pop up at the end of scenario).
    - The following exceptions apply:
        - The tool expects a StatusNotification(Unavailable) per connector from the Charging Station before updating firmware. But when a Charging Station supports updating firmware during a transaction, it is allowed remain Available and not send the StatusNotification(Unavailable).
        - For the OCTT test cases 037_1, 037_2 and 037_3, the StatusNotification(Charging) is optional.
        - For the OCTT test cases 038 and 039, the StatusNotification(Finishing) is optional.
        - For the OCTT test cases 015: if the Charging Station sends a StatusNotification(Unavailable) instead of StatusNotification(Finishing) before resetting this may be considered as correct behavior.
        - For the OCTT test cases 016: if the Charging Station does not send a StatusNotification(Finishing) before resetting this may be considered as correct behavior.
- If an unexpected StatusNotification is received by the OCPP Compliance Testing Tool, the result should *only* be approved (click Yes in pop up at the end of scenario) if it is a "*valid*" StatusNotification. The rules for determining whether it is "*valid*" are the following:
    - When waiting for a certain set of messages, it is allowed to first receive some specified StatusNotification messages.
        - When testing a testcase from "Reservation" AND the Charging Station has multiple connectors connected to one EVSE, then it is allowed to send StatusNotification messages for the other connected connector(s) with either the status; Available, Reserved, Preparing, Unavailable.
            - Any other StatusNotification message with an unexpected connectorId (except connectorId 0) is incorrect.
        - An unexpected StatusNotification message with connectorId 0 should contain an ErrorCode (Other than "NoError") or Info to be valid. If a test would fail because of such a StatusNotification, the test should be retested.

        - The following StatusNotification messages with the expected connectorId, but an unexpected status are valid:
            - Waiting for StartTransaction.req or StopTransaction.req, but first receiving StatusNotification(SuspendedEV) and / or StatusNotification(SuspendedEVSE).
            - After a (re)boot waiting for StatusNotification(Available), but first receiving StatusNotification(Unavailable).
    - It is NOT allowed to send two duplicate StatusNotification messages after one another, looking at the combination of the following fields: ConnectorId, Status, ErrorCode, Info. So if one or more of these fields is different, then the message is valid. For example: When receiving a StatusNotification with a duplicate Status, ConnectorId and ErrorCode, but there is extra info included at "Info" field, then the message is valid.

- If previous rule has been applied and the OCTT result is “PASS“ the scenario is considered successfully executed.
- If the previous rules have been applied and the OCTT result is “FAIL“
    - If one or more tool validations have failed, the result of the scenario is considered as failed.
    - If the test case is not executed according to the scenario, the result of the scenario is considered as failed.
    - Otherwise, a retest of the scenario should be executed to make sure that it is not due to the test setup or human error.

Appendix E: Example EVs to use for testing

The following list contains example EVs that can be used for testing (non exhaustive):

Socket type	Possible EV (non-exhaustive list)
CHAdeMO	Citroën Berlingo Electric Citroën C-Zero Kia Soul EV Mitsubishi Outlander PHEV Nissan Leaf 2 or e-NV200
CCS	BWM i3 Hyundai Ioniq Hyundai KONA Kia e-Niro Opel Ampera-e Tesla Model 3 Volkswagen e-Golf or e-up
Tesla	Tesla model S / X